Des. Codes Cryptogr. (2015) 74:31–40
DOI 10.1007/s10623-013-9849-9

New bounds on $\bar{2}$-separable codes of length 2

Minquan Cheng · Hung-Lin Fu · Jing Jiang · Yuan-Hsun Lo · Ying Miao

Received: 4 March 2013 / Revised: 10 June 2013 / Accepted: 12 June 2013 /
Published online: 27 June 2013

Abstract Let $\mathbb{C}$ be a code of length n over an alphabet of q letters. The descendant code $\mathsf{desc}(\mathbb{C}_0)$ of $\mathbb{C}_0 = \{\mathbf{c}^1, \mathbf{c}^2, \ldots, \mathbf{c}^t\} \subseteq \mathbb{C}$ is defined to be the set of words $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ such that $x_i \in \{c_i^1, c_i^2, \ldots, c_i^t\}$ for all $i = 1, \ldots, n$. $\mathbb{C}$ is a $\bar{t}$-separable code if for any two distinct $\mathbb{C}_1, \mathbb{C}_2 \subseteq \mathbb{C}$ such that $|\mathbb{C}_1| \leq t$, $|\mathbb{C}_2| \leq t$, we always have $\mathsf{desc}(\mathbb{C}_1) \neq \mathsf{desc}(\mathbb{C}_2)$. The study of separable codes is motivated by questions about multimedia fingerprinting for protecting copyrighted multimedia data. Let $M(\bar{t}, n, q)$ be the maximal possible size of such a separable code. In this paper, we provide an improved upper bound for $M(\bar{2}, 2, q)$ by a graph theoretical approach, and a new lower bound for $M(\bar{2}, 2, q)$ by deleting suitable points and lines from a projective plane, which coincides with the improved upper bound in some

Communicated by C. J. Colbourn.

M. Cheng (✉)
Department of Mathematical Sciences, Guangxi Normal University,
Guilin 541004, People's Republic of China
e-mail: chengqinshi@hotmail.com

H.-L. Fu
Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan
e-mail: hlfu@math.nctu.edu.tw

J. Jiang
Graduate School of Systems and Information Engineering, University of Tsukuba,
Tsukuba, Ibaraki 305-8573, Japan
e-mail: jjiang2008@hotmail.com

Y.-H. Lo
Department of Applied Mathematics, National University of Kaohsiung, Kaohsiung 811, Taiwan
e-mail: yhlo0830@gmail.com

Y. Miao
Faculty of Engineering, Information and Systems, University of Tsukuba,
Tsukuba, Ibaraki 305-8573, Japan
e-mail: miao@sk.tsukuba.ac.jp

places. This corresponds to the bounds of maximum size of bipartite graphs with girth 6 and a construction of such maximal bipartite graphs.

Keywords Multimedia fingerprinting · Separable code · 4-Cycle free bipartite graph · Zarankiewicz number · Projective plane

Mathematics Subject Classification 94B25 · 94A62 · 05B40 · 05C51 · 05B25

1 Introduction

Let n, M and q be positive integers, and Q an alphabet with $|Q| = q$. A set $\mathbb{C} = \{\mathbf{c}^1, \mathbf{c}^2, \ldots, \mathbf{c}^M\} \subseteq Q^n$ is called an (n, M, q) code and each $\mathbf{c}^i$ is called a codeword. Without loss of generality, we may assume $Q = \{0, 1, \ldots, q-1\}$.

For any subset of codewords $\mathbb{C}_0 \subseteq \mathbb{C}$, we define the set of ith coordinates of $\mathbb{C}_0$ as

$$\mathbb{C}_0(i) = \{c_i \in Q | \mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{C}_0\}, \quad 1 \le i \le n,$$

and the descendant code of $\mathbb{C}_0$ as

$$\mathsf{desc}(\mathbb{C}_0) = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) \in Q^n \mid x_i \in \mathbb{C}_0(i), \quad 1 \le i \le n\},$$

that is,

$$\mathsf{desc}(\mathbb{C}_0) = \mathbb{C}_0(1) \times \mathbb{C}_0(2) \times \cdots \times \mathbb{C}_0(n).$$

Definition 1.1 Suppose $\mathbb{C}$ is an (n, M, q) code and $t \ge 2$ is an integer. $\mathbb{C}$ is a $\bar{t}$-separable code, or $\bar{t}$-SC(n, M, q) in short, if for any $\mathbb{C}_1, \mathbb{C}_2 \subseteq \mathbb{C}$ such that $|\mathbb{C}_1| \le t$, $|\mathbb{C}_2| \le t$ and $\mathbb{C}_1 \ne \mathbb{C}_2$, we always have $\mathsf{desc}(\mathbb{C}_1) \ne \mathsf{desc}(\mathbb{C}_2)$, that is, there is at least one coordinate i, $1 \le i \le n$, such that $\mathbb{C}_1(i) \ne \mathbb{C}_2(i)$.

Let $M(\bar{t}, n, q) = \max\{M \mid \text{there exists a } \bar{t}\text{-SC}(n, M, q)\}$. A $\bar{t}$-SC(n, M, q) is said to be optimal if $M = M(\bar{t}, n, q)$, and asymptotically optimal if $\lim\limits_{q\to\infty} \dfrac{M}{M(\bar{t}, n, q)} = 1$.

The study of separable codes is motivated by questions about multimedia fingerprinting which can effectively trace and even identify the sources of pirate copies of copyrighted multimedia data, see, e.g., [6,19]. It is not difficult to see [6] that identifiable parent property codes [15,24], frameproof codes [2,4], perfect hash families [20,25] and some other structures in digital fingerprinting all imply separable codes.

In multimedia fingerprinting, $\mathsf{desc}(\mathbb{C}_0)$ consists of all the n-tuples that could be produced by a coalition holding the codewords in $\mathbb{C}_0$, where the length n corresponds to the number of orthogonal basis signals in the multimedia content. Since the size M of $\bar{t}$-SC(n, M, q) corresponds to the number of fingerprints assigned to authorized users, we should try to construct separable codes with size M as large as possible, given length n. Cheng and Miao [6] showed that long-length separable codes can be constructed by concatenating short-length separable codes. This stimulates the investigation of separable codes with length $n = 2$.

In [7] an upper bound on $M(\bar{2}, 2, q)$ was derived, and two infinite series of optimal $\bar{2}$-$(2, M, q)$-SCs were constructed.

Theorem 1.2 [7] *For any positive integer q, $M(\overline{2}, 2, q) \leq qk + t$, where $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$, and*

$$t = \begin{cases} \lfloor \frac{q(q-1-k^2+k)}{2k} \rfloor, & \text{if } k^2 - k + 1 \leq q \leq k^2; \\ \lfloor \frac{qk}{(k+1)^2 - q} \rfloor, & \text{if } k^2 + 1 \leq q \leq k^2 + k. \end{cases}$$

Furthermore, $M(\overline{2}, 2, q) = qk + t$ if $q = k^2 - k + 1$ for any prime power $k - 1 \geq 2$ and $q = k^2 + k$ for any prime power $k \geq 2$.

In this paper, by using graph theoretical terminologies, we obtain a tighter upper bound on $M(\overline{2}, 2, q)$. By using projective geometrical terminologies, we also obtain a lower bound on $M(\overline{2}, 2, q)$, parts of which agree with the new derived upper bound. In other words, we construct several new infinite series of optimal $\overline{2}$-$(2, M, q)$-SCs.

2 Related combinatorial objects

In order to investigate separable codes, in this section, we describe several related combinatorial structures.

For any $(2, M, q)$ code $\mathbb{C}$ defined on $Q = \{0, 1, \ldots, q-1\}$, we define A_i for $i \in Q$ as $A_i = \{x_2 \mid (x_1, x_2) \in \mathbb{C},\ x_1 = i\}$. Obviously, $A_i \subseteq Q$ holds for any $i \in Q$, and $|A_0| + |A_1| + \cdots + |A_{q-1}| = M$.

Definition 2.1 Let K be a subset of non-negative integers, and v, b be two positive integers. A generalized $(v, b, K, 1)$ packing is a pair $(X, \mathbb{B})$ where X is a set of v elements and $\mathbb{B}$ is a set of b subsets of X called blocks that satisfy

(1) $|B| \in K$ for any $B \in \mathbb{B}$;
(2) every pair of distinct elements of X occurs in at most one block of $\mathbb{B}$.

Cheng et al. [7] showed a relationship between separable codes and generalized packings.

Lemma 2.2 [7] *There exists a $\overline{2}$-SC$(2, M, q)$ defined on Q if and only if there exists a generalized $(q, q, K, 1)$ packing $(Q, \{A_0, A_1, \ldots, A_{q-1}\})$, with $K = \{|A_0|, |A_1|, \ldots, |A_{q-1}|\}$, and $M = |A_0| + |A_1| + \cdots + |A_{q-1}|$.*

A generalized $(q, q, \{k\}, 1)$ packing can be constructed by developing a near difference set. A $(q, k, 1)$ near difference set defined on an additively written group G of order $|G| = q$ is a k-subset D of G such that the differences $\{x - y \mid x, y \in D, x \neq y\}$ contains $k(k-1)$ distinct elements of G.

Lemma 2.3 *For any integer $k \geq 2$, let $q \geq k^2 - k + 1$. If there exists a $(q, k, 1)$ near difference set, then there exists a generalized $(q, q, \{k\}, 1)$ packing.*

Proof Let D be a $(q, k, 1)$ near difference set defined on an additively written group G. For any $g \in G$, define $D + g = \{x + g \mid x \in D\}$ and $\mathbb{B} = \{D + g \mid g \in G\}$. Then $(G, \mathbb{B})$ is the desired generalized $(q, q, \{k\}, 1)$ packing. □

Near difference sets are not easy to construct. However, a $(k^2+k+1, k, 1)$ near difference set always exists [23] for any prime power k. This Singer difference set generates a generalized $(k^2 + k + 1, k^2 + k + 1, \{k\}, 1)$ packing, which corresponds to an optimal $\overline{2} - \mathrm{SC}(2, (k + 1)(k^2 + k + 1), k^2 + k + 1)$ described in Theorem 1.2.

Given a generalized $(v, b, K, 1)$ packing $(Q, \mathbb{B})$, we can define its associated element-block graph as the bipartite graph $G_{Q,\mathbb{B}}$ with vertex partition Q and $\mathbb{B}$ such that $x \in Q$ is adjacent to $B \in \mathbb{B}$ if and only if $x \in B$. It is clear that the corresponding element-block graph of a generalized $(v, b, K, 1)$ packing $(Q, \mathbb{B})$ is a C_4-free bipartite subgraph of $K_{v,b}$, because any pair of distinct elements of Q can occur in at most one block of $\mathbb{B}$. In other words, the girth of this bipartite graph is at least 6, where the girth of a graph is the length of a shortest cycle contained in the graph.

Zarankiewicz numbers [27] involve bounds on the maximum number of edges in a bipartite graph without a particular subgraph. We denote by $z(m, n; s, t)$, $m \leq n$ and $s \leq t$, the maximum number of edges in a subgraph of $K_{m,n}$ that does not contain a subgraph isomorphic to $K_{s,t}$. In particular, when $m = n$ and $s = t$, simply put $z(n; t) = z(n, n; t, t)$. It is clear that $z(q; 2)$, which is the maximum size of a C_4-free bipartite subgraph of $K_{q,q}$, is equals to $M(\overline{2}, 2, q)$ by Lemma 2.2. Meanwhile, García-Vázquez et al. [11] stated that any C_4-free bipartite subgraph of $K_{q,q}$ with size $z(q; 2)$ must have girth 6. Therefore, our problem is equivalent to finding the maximum size of bipartite graphs with girth 6, where the size of a graph refers to the number of edges it contains, and constructing such maximal bipartite graphs.

We can see our problem in one more way. Given a generalized $(q, q, K, 1)$ packing $(Q, \mathbb{B})$, if we define two elements of Q are adjacent in $B \in \mathbb{B}$ if they occur in the same block B, then each block can be seen as a clique of order $|B|$ belonging to K. Since each pair of distinct elements of Q occurs in a block of $\mathbb{B}$ at most once, this generalized $(q, q, K, 1)$ packing can be viewed as a packing of K_q by q cliques of orders belonging to K. Therefore, in order to evaluate $z(q; 2) = M(\overline{2}, 2, q)$, it is sufficient to pack K_q by q cliques so that the sum of order of the q cliques is maximum.

It is well known [3] that $z(q; 2) \leq (q + q\sqrt{4q-3})/2$ and the equality holds when $q = k^2 + k + 1$ for any prime power k. Goddard et al. [12] found the exact values of $z(q; 2)$ for $q \leq 10$. Very recently, Damásdi et al. [8] also found the exact values of $z(q; 2)$ for $q = k^2 + k - 2, k^2 + k - 1$ with k being a prime power, among others. Theorem 1.2 is an improvement of the results made by Cheng et al. [7]. It is also known [3] that if q is sufficiently large then

$$q^{3/2} - q^{4/3} < z(q; 2) \leq (q + q\sqrt{4q-3})/2;$$

In particular, $\lim_{q\to\infty} \dfrac{z(q; 2)}{q^{3/2}} = 1$. For the up-to-date information on Zarankiewicz numbers, the reader is referred to [8].

3 Upper bound

Bipartite graphs with high girth and their related graphs have been extensively investigated, see, e.g., [1,8–11,13,16–18,21,22,26]. We start this section with the following proposition.

Proposition 3.1 [5] *Suppose $(X, \mathbb{B})$ is a generalized $(v, b, \{k, k+1\}, 1)$ packing, for some k, with $\mathbb{B} = \{B_1, B_2, \ldots, B_b\}$. If $\binom{v}{2} - \sum_{i=1}^{b} \binom{|B_i|}{2} < k$, then $G_{X,\mathbb{B}}$, the element-block graph of $(X, \mathbb{B})$, is a C_4-free subgraph of $K_{v,b}$ with maximum size.*

If K_q can be packed by q cliques $K_{x_1}, K_{x_2}, \ldots, K_{x_q}$ with leave L, where $x_i \leq x_j$ for $1 \leq i < j \leq q$, then we say K_q admits a feasible $(x_1, x_2, \ldots, x_q)$ packing with leave L. For convenience, we replace $(x_1, x_2, \ldots, x_q)$ packing by $(k^{q-t}, (k+1)^t)$ packing when

$$k = x_1 = \cdots = x_{q-t} \text{ and } x_{q-t+1} = \cdots = x_q = k+1$$

for some $k \in \mathbb{N}$ and $1 \leq t \leq q$. For any $(k^{q-t}, (k+1)^t)$ packing $\mathcal{P}$ of K_q, we have

$$q\binom{k}{2} \leq (q-t)\binom{k}{2} + t\binom{k+1}{2} \leq \binom{q}{2},$$

which implies $k \leq \frac{1+\sqrt{4q-3}}{2}$. In order to maximize $\sum_{i=1}^{q} x_i$ which subjects to an $(x_1, x_2, \ldots, x_q)$ packing, Proposition 3.1 promises to consider a feasible $(k^{q-t}, (k+1)^t)$ packing with $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$ and $|L| < k$. Therefore, our objective is to find the maximum index t. Note that $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$ implies $k^2 - k + 1 \leq q < k^2 + k + 1$. In this section, we investigate $z(q; 2)$ by fixing the index k and then classifying q, from $k^2 - k + 1$ to $k^2 + k$, into several cases. The following Theorem 3.2 is contained in Theorem 1.2.

Theorem 3.2 [3,7] *For any prime power* $k - 1 \geq 2$, $z(k^2 - k + 1; 2) = k^3 - k^2 + k$. *For any prime power* $k \geq 2$, $z(k^2 + k; 2) = k^3 + 2k^2$.

Theorem 3.3 *For any* $k^2 + 1 \leq q \leq k^2 + k - 2$ *and* $k \geq 2$, *we have*

$$z(q; 2) \leq qk + \left\lfloor \frac{(k-1)q}{(k+1)^2 - (q+1)} \right\rfloor.$$

Proof Let $q = k^2 + k - s$, $s = 2, 3, \ldots, k-1$. Assume $\mathcal{P}$ is a $(k^{q-t}, (k+1)^t)$ packing of K_q, where $0 \leq t \leq q - 1$. We claim by contradiction that $t \leq \lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \rfloor$. That is, suppose $t > \lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \rfloor$.

For $i \geq 0$, let r_i be the number of vertices that is contained in exactly i cliques of order $k+1$ in $\mathcal{P}$. Since the degree of each vertex is $k^2+k-s-1$, trivially $r_i = 0$ for all $i > k$. We now claim $r_k = 0$. Suppose not, that is, there exists a vertex v contained in exactly k cliques of order $k+1$, say $C_1, C_2, \ldots, C_k$. Let $A = \{v\} \cup \bigcup_{i=1}^{k} V(C_i)$ and $B = V(K_q) \setminus A$, where $V(G)$ is the vertex set of graph G. Since there is no other subgraph isomorphic to K_{k+1} out of A except $C_1, C_2, \ldots, C_k$, each of the remaining cliques of order $k+1$ must contain at least one vertex in B. That is, each of such cliques needs at least k edges between A and B. Therefore, we have at most $k + \lfloor \frac{(k^2+1)(k-s-1)}{k} \rfloor$ cliques of order $k+1$. Thus,

$$k(k-s) \geq k + \left\lfloor \frac{(k^2+1)(k-s-1)}{k} \right\rfloor \geq t > \left\lfloor \frac{(k-1)q}{(k+1)^2 - (q+1)} \right\rfloor.$$

This implies $ks^2 - ks - k + s < 0$, so $ks(s-1) \leq k - s < k$, that is, $s(s-1) < 1$, which contradicts $2 \leq s \leq k-1$. So $r_k = 0$.

Consider the number of ordered pairs (v, C), where v is a vertex in the clique C of order $k+1$ in $\mathcal{P}$. Under our assumption, there are exactly t cliques of order $k+1$, then

$$t(k+1) = (k-1)r_{k-1} + (k-2)r_{k-2} + \cdots + (k-s)r_{k-s} + \cdots + r_1. \tag{1}$$

This implies that

$$t(k+1) \leq (k-1)(r_{k-1} + \cdots + r_{k-s+1}) + (k-s)(q - (r_{k-1} + \cdots + r_{k-s+1})),$$

so

$$\frac{t(k+1) - q(k-s)}{s-1} \leq r_{k-1} + \cdots + r_{k-s+1}. \tag{2}$$

Now, we drop all the t cliques of order $k+1$ from K_q. Denote by G the remaining subgraph. We again consider the number of ordered pairs (v', C'), where v' is a vertex in the clique C' of order k in $\mathcal{P}$. On one hand there are exactly $q-t$ cliques of order k, and on the other hand there are exactly r_i vertices of degree $q-1-ki$, for $i = 0, 1, \ldots, k-1$. Since the vertex of degree $q-1-ki$ can be contained in at most $\frac{q-1-ki}{k-1}$ cliques of order k, we have

$$(q-t)k \leq r_{k-1} + 2r_{k-2} + \cdots + (s-1)r_{k-s+1} + (s+1)r_{k-s} + \cdots + (k+1)r_0. \quad (3)$$

Combining (1) and (3) we have

$$t(k+1) + (q-t)k \leq k(r_{k-1} + \cdots + r_{k-s+1}) + (k+1)(q - (r_{k-1} + \cdots + r_{k-s+1})),$$

and thus

$$r_{k-1} + \cdots + r_{k-s+1} \leq q - t. \quad (4)$$

Finally, (2) and (4) imply that $t \leq \frac{q(k-1)}{k+s} = \frac{(k-1)q}{(k+1)^2-(q+1)}$, a contradiction to the hypothesis. Thus we complete the proof. □

Theorem 3.4 *For any $q = k^2$ with $k \geq 2$, we have*

$$z(q;2) \leq qk + \left\lfloor \frac{(3k^2+k-1) - \sqrt{5k^4+6k^3-k^2-2k+1}}{2} \right\rfloor.$$

Proof Assume $\mathcal{P}$ is a $(k^{q-t}, (k+1)^t)$ packing of K_q. For $i \geq 0$, let r_i be the number of vertices that is contained in exactly i cliques of order $k+1$ in $\mathcal{P}$. Since $q = k^2$, we have $r_i = 0$ for all $i \geq k$. Similar to the Proof of Theorem 3.3, we first consider the number of ordered pairs (v, C), where v is a vertex in the clique C of order $k+1$ in $\mathcal{P}$. Then after dropping those cliques of order $k+1$, we consider the number of ordered pairs (v', C'), where v' is a vertex in the clique C' of order k in $\mathcal{P}$. Note that in the remaining graph after dropping t cliques of order $k+1$, there are exactly r_i vertices of degree $k^2 - ik - 1$. Then we have

$$\begin{cases} t(k+1) = (k-1)r_{k-1} + \cdots + 2r_2 + r_1 \\ (q-t)k \leq r_{k-1} + \cdots + (k-2)r_2 + (k-1)r_1 + (k+1)r_0 \end{cases}$$

which implies $t \leq r_0$. This concludes that the t cliques of order $k+1$ are out of at most $k^2 - t$ vertices somewhere in $\mathcal{P}$. We immediately have

$$t\binom{k+1}{2} \leq \binom{k^2-t}{2}.$$

That is,

$$t^2 + (1-k-3k^2)t + (k^4 - k^2) \geq 0.$$

Since $t \leq k^2$, the above inequality is true only when $t \leq \frac{(3k^2+k-1)-\sqrt{5k^4+6k^3-k^2-2k+1}}{2}$. Hence we complete the proof. □

Theorem 3.5 *For any $k^2 - k + 2 \leq q \leq k^2 - 1$ and $k \geq 2$, we have $z(q;2) \leq qk$.*

Proof Let $q = k^2 - s$, where $s = 1, 2, \ldots, k-2$. Assume $\mathcal{P}$ is a $(k^{q-t}, (k+1)^t)$ packing of K_q. Suppose $t \geq 1$. Define G to be the graph by dropping one of the cliques of order $k+1$, say $\widehat{K}$, from K_q. Let $A \subseteq V(G)$ be the collection of vertices whose degree is equal to $q-1-k$, and $B = V(G) \setminus A$. Note that $|A| = k+1$ and $|B| = q-k-1$. Now, consider the number of ordered pairs (v, C), where v is a vertex in the clique C in $\mathcal{P}$ different from

$\widehat{K}$. Notice that for each $v \in A$, $\deg_G(v) = k^2 - s - 1 - k = (k-1)^2 + (k-s-2)$, then v is contained in at most $k-1$ cliques different from $\widehat{K}$. Similarly, each vertex in B can be contained in at most k cliques. By counting the number of pairs (v, C), we have

$$(t-1)(k+1) + (q-t)k \le (k+1)(k-1) + (q-k-1)k.$$

This implies that $t \le 0$, a contradiction occurs. Thus the result follows. □

4 Lower bound

Now we derive a lower bound on $z(q; 2) = M(\bar{2}, 2, q)$ via projective planes. A projective plane consists of a set of lines, a set of points, and a relation between points and lines called incidence, having the following properties:

(1) Given any two distinct points, there is exactly one line incident with both of them.
(2) Given any two distinct lines, there is exactly one point incident with both of them.
(3) There are four points such that no line is incident with more than two of them.

Clearly, a projective plane of order k is a generalized $(k^2+k+1, k^2+k+1, \{k+1\}, 1)$ packing $(X, \mathbb{B})$ in which every pair of distinct elements of X occurs in exactly one block of $\mathbb{B}$. It is well-known [14] that a projective plane of order k always exists for any prime power k.

Theorem 4.1 *For any prime power $k \ge 2$, let $k^2 - 1 \le q \le k^2 + k - 1$. Then there exists a generalized $(q, q, \{k, k+1\}, 1)$ packing, $(X', \mathbb{B}')$, with $|X'| = |\mathbb{B}'| = q$ such that exactly $k^3 - k^2 - k - qk + 2q + 1$ blocks out of $\mathbb{B}'$ are of size k. That is,*

$$z(q; 2) \ge 2qk - k^3 + k^2 + k - q - 1.$$

Proof We start from a projective plane of order k, $(X, \mathbb{B})$. Note that $|X| = |\mathbb{B}| = k^2 + k + 1$, and for any $B \in \mathbb{B}$, $|B| = k + 1$. Pick an arbitrary point $a \in X$ and an arbitrary line $B^* = \{x_1, x_2, \ldots, x_{k+1}\} \in \mathbb{B}$ which does not contain the point a. For each $i = 1, \ldots, k+1$, let $B_i \in \mathbb{B}$ be the line containing the points a and x_i. Let $2 \le s \le k+2$. Dropping s lines $B^*, B_1, \ldots, B_{s-1}$ and s points $a, x_1, \ldots, x_{s-1}$ from $(X, \mathbb{B})$, we obtain a generalized $(q, q, \{k, k+1\}, 1)$ packing, $(X', \mathbb{B}')$, with $q = k^2 + k + 1 - s$, $X' = X \setminus \{a, x_1, \ldots, x_{s-1}\}$, $\mathbb{B}' = \mathbb{B} \setminus \{B^*, B_1, \ldots, B_{s-1}\}$, having $\Delta = (s-1)(k-1) + (k+1-s+1) = k^3 - k^2 - k - qk + 2q + 1$ blocks of size k and $k^2 + k + 1 - \Delta - s$ blocks of size $k+1$. Therefore, $z(q; 2) \ge k\Delta + (k+1)(k^2 + k + 1 - \Delta - s) = 2qk - k^3 + k^2 + k - q - 1$. □

Applying Theorems 1.2, 3.3 and 3.5, we immediately have the following result.

Corollary 4.2 *For any prime power $k \ge 2$, $z(k^2 - 1; 2) = k^3 - k$, $z(k^2 + k - 2; 2) = k^3 + 2k^2 - 4k + 1$, $z(k^2 + k - 1; 2) = k^3 + 2k^2 - 2k$.*

We remark that Damaásdi et al. [8] obtained independently the same results for $q = k^2 + k - 2, k^2 + k - 1$ in Corollary 4.2. It is easy to verify that the corresponding $\bar{2}$-SC$(2, M, q)$s constructed in Theorem 4.1 are asymptotically optimal for all $k^2 - 1 \le q \le k^2 + k - 1$ with prime power k. The lower bound described in Theorem 4.1 is better than $q^{3/2} - q^{4/3}$ described in [3] for any prime power k.

5 Summary

The main results in the previous sections can be summarized in the following theorem.

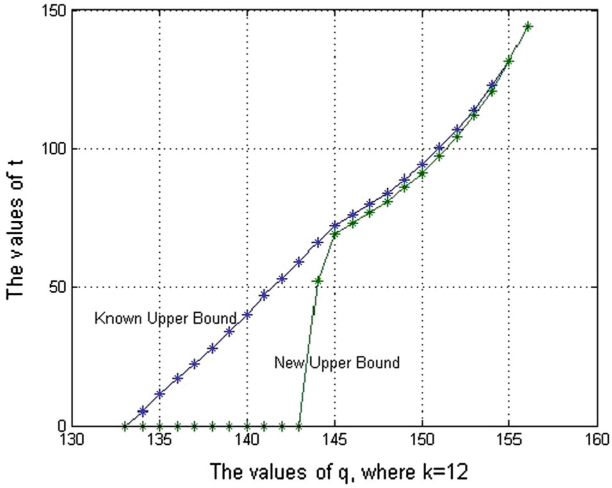

Fig. 1 Bounds for $k = 12$

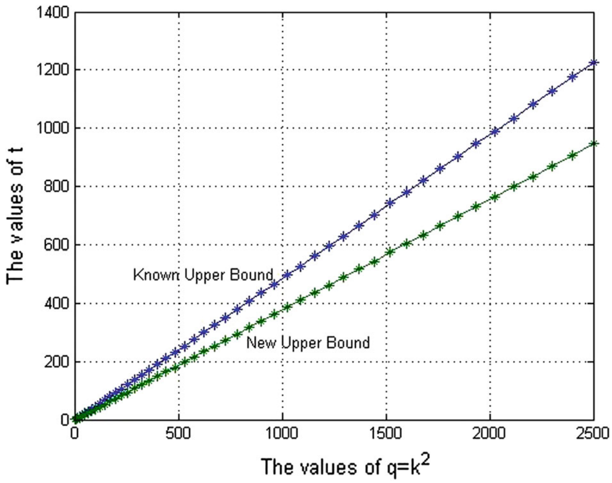

Fig. 2 Bounds for $q = k^2$

Theorem 5.1 *For any positive integer* q, $M(\overline{2}, 2, q) \leq qk + t$, *where* $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$, *and*

$$t = \begin{cases} 0 & \text{if } k^2 - k + 1 \leq q \leq k^2 - 1; \\ \left\lfloor \frac{(3k^2+k-1)-\sqrt{5k^4+6k^3-k^2-2k+1}}{2} \right\rfloor & \text{if } q = k^2; \\ \left\lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \right\rfloor & \text{if } k^2 + 1 \leq q \leq k^2 + k - 2; \\ k^2 - k & \text{if } q = k^2 + k - 1; \\ k^2 & \text{if } q = k^2 + k. \end{cases}$$

Furthermore, $M(\overline{2}, 2, q) = qk + t$ *if* $q = k^2 - k + 1$ *for any prime power* $k - 1 \geq 2$, *and* $q = k^2 - 1, k^2 + k - 2, k^2 + k - 1, k^2 + k$ *for any prime power* $k \geq 2$.

The above Figs. 1 and 2 illustrate our improvement on the upper bound of $M(\overline{2}, 2, q)$. Figure 1 depicts the known upper bound given in [7] and the new upper bound given in Theorem 5.1 when $k = 12$, while Fig. 2 depicts those upper bounds when $q = k^2$. It can be seen that our new upper bound is much tighter than the known upper bound.

Acknowledgments The interesting paper [8] was drawn to the authors' attention by one of the two anonymous reviewers. The authors express their sincere thanks to the reviewers for their valuable comments and suggestions in revising this paper. Cheng is supported by Guangxi Natural Science Foundation under Grant No. 2013GXNSFCA019001, by the general scientific research project of the Education Department of Guangxi Province (Grant No. 2013YB039), and by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry. Fu and Lo are supported by NSC 100-2115-M-009-005-MY3. Miao is supported by JSPS Grant-in-Aid for Scientific Research (C) under Grant No. 24540111.

References

1. Benson C.T.: Minimal regular graphs of girths eight and twelve. Can. J. Math. **18**, 1091–1094 (1966).
2. Blackburn S.R.: Frameproof codes. SIAM J. Discret. Math. **16**, 499–510 (2003).
3. Bollobás B.: Extremal Graph Theory. Academic Press, New York (1978).
4. Boneh D., Shaw J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inf. Theory **44**, 1897–1905 (1998).
5. Bryant D.E., Fu H.L.: C_4-saturated bipartite graphs. Discret. Math. **259**, 263–268 (2002).
6. Cheng M., Miao Y.: On anti-collusion codes and detection algorithms for multimedia fingerprinting. IEEE Trans. Inf. Theory **57**, 4843–4851 (2011).
7. Cheng M., Ji L., Miao Y.: Separable codes. IEEE Trans. Inf. Theory **58**, 1791–1803 (2012).
8. Damásdi G., Héger H., Szönyi T.: Cages, geometries and Zarankiewicz' problem. Ann. Univ. Eőtvős Loránd (2013).
9. de Caen D., Székely L.A.: On dense bipartite graphs of girth eight and upper bounds for certain configurations in planar point–line systems. J. Comb. Theory Ser. A **77**, 268–278 (1997).
10. Erdős P., Sárkőzy A., Sós V.T.: On product representations of powers. I. Eur. J. Comb. **16**, 567–588 (1995).
11. García-Vázquez P., Balbuena C., Marcote X., Valenzuela J.C.: On extremal bipartite graphs with high girth. Electron. Notes Discret. Math. **26**, 67–73 (2006).
12. Goddard W., Henning M.A., Oellermann O.R.: Bipartite Ramsey numbers and Zarankiewicz numbers. Discret. Math. **219**, 85–95 (2000).
13. Györi E.: C_6-free bipartite graphs and product representations of squares. Discret. Math. **165**(166), 371–375 (1997).
14. Hirschfeld J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Oxford Science, Oxford (1998).
15. Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.: On codes with the identifiable parent property. J. Comb. Theory Ser. A **82**, 121–133 (1998).
16. Hoory S.: The size of bipartite graphs with a given girth. J. Comb. Theory Ser. B **86**, 215–220 (2002).
17. Lam T.: Graphs without cycles of even length. Bull. Australas. Math. Soc. **63**, 435–440 (2001).
18. Lam T.: A result on $2k$-cycle-free bipartite graphs. Australas. J. Comb. **32**, 163–170 (2005).
19. Liu K.J.R., Trappe W., Wang Z.J., Wu M., Zhao H.: Multimedia Fingerprinting Forensics for Traitor Tracing. Hindawi Publishing Corporation, New York (2005).
20. Mehlhorn K.: Data Structures and Algorithms 1. Springer, Berlin (1984).
21. Naor A., Verstraëthe J.: A note on bipartite graphs without $2k$-cycles. Comb. Probab. Comput. **14**, 845–849 (2005).
22. Neuwirth S.: The size of bipartite graphs with girth eight, arXiv:math/0102210 (2001).
23. Singer J.: A theorem in finite projective geometry and some applications to number theory. Trans. Am. Math. Soc. **43**, 377–385 (1938).
24. Staddon J.N., Stinson D.R., Wei R.: Combinatorial properties of frameproof and traceability codes. IEEE Trans. Inf. Theory **47**, 1042–1049 (2001).

25. Stinson D.R., van Trung, T., Wei R.: Secure frameproof codes, key distribution pattern, group testing algorithms and related structures. J. Stat. Plan. Inference **86**, 595–617 (2000).
26. Wenger R.: Extremal graphs with no C^4's, C^6's, or C^{10}'s. J. Comb. Theory Ser. B **52**, 113–116 (1991).
27. Zarankiewicz K.: Problem P101. Colloquium Math. **2**, 301 (1951).